VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

NÁSTROJ PRO TESTOVANÍ BEZPEČNOSTI WIFI SÍTÍ

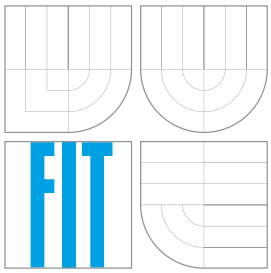
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

MARTIN HALA

BRNO 2011

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

NÁSTROJ PRO TESTOVANÍ BEZPEČNOSTI WIFI SÍTÍ

SECURITY TOOL FOR WIFI NETWORK

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — MARTIN HALA
AUTHOR

VEDOUCÍ PRÁCE — Ing. MATEJ KAČIC
SUPERVISOR

BRNO 2011

Abstrakt

Hlavním cílem tohoto nástroje je testování úrovně zabezpečení Wi-Fi sítí, jak pro domácí, tak pro firemní účely. Vychází se z nejaktuálnějších bezpečnostních znalostí o bezdrátových sítích. Hlavní cíle jsou následující: Přenositelnost - implementováno v live linuxové distribuci, jednoduché ovládání - přehledné GUI, testování - širší možnosti výběru testů, vyhodnocení úrovně zabezpečení - doporučení vyplývající ze standardu NIST.

Abstract

The main purpose of this tool is testing wireless networks security level for both personal and commercial use. It is based on latest knowledge about security of wireless networks. Key features are: portability - implemented on live linux distro, simple manipulation - well aranged GUI, testing - rich options of tests selection, security level evaluation - recommendations consequent on NIST standard.

Klíčová slova

Bezpečnost bezdrátových sítí, Wi-Fi, WST, testovací nástroj, aircrack-ng, síťová sonda.

Keywords

wireless security, Wi-Fi, WST, testing tool, aircrack-ng, network sniffer.

Citace

Martin Hala: Nástroj pro testovaní bezpečnosti wifi sítí, bakalářská práce, Brno, FIT VUT v Brně, 2011

Nástroj pro testovaní bezpečnosti wifi sítí

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Mateje Kačice.

.....
Martin Hala
18. května 2011

Poděkování

Chtěl bych mnohokrát poděkovat vedoucímu mé bakalářské práce, panu Ing. Mateji Kačicovi za veškeré připomínky, odborné rady a dobré nápady při vytváření nástroje.

Obsah

Kapitola 1

Úvod

Většina firem v současnosti se jen stěží dokáže obejít bez Wi-Fi sítí. Stoupající zájem o Wi-Fi sítě se projevuje i u domácích uživatelů, kteří je využívají pro připojení svých bezdrátových zařízení. Tato technologie je v posledních letech velmi oblíbená a snadno dostupná i pro běžné uživatele, kteří nemají dostatečné znalosti na jejich kvalitní zabezpečení.

Právě nedostačující úroveň zabezpečení je jednou z hlavních iniciativ pro vytvoření nástroje, který bude administrátora sítě kontrolovat, zda nastavená bezpečnostní úroveň je dostatečná.

Ve druhé kapitole se práce zábývá teoretickým úvodem. Popisuje Wi-Fi jako standard. Dále se zmiňuje o základních informacích jako je rozdělení z geografického hlediska či princip přenosu dat na fyzické a linkové vrstvě. V závěru kapitoly je zmínka o nejznámějších standardech IEEE 802.11.

Analýzou problémů se zabývá třetí kapitola. Zmiňuje se o základních bezpečnostních funkcích a pokračuje výpisem jednotlivých bezpečnostních rizik. Analyzuje Wi-Fi síť z hlediska bezpečnosti a dopodrobna popisuje jednotlivá bezpečnostní rizika a známé útoky. Na konci je zmínka o existujících nástrojích.

Požadavky aplikace, je název úvodní části kapitoly s názven Návrh aplikace, která je jako čtvrtá. Po podrobném popisu požadavků následují informace o funkci nástroje, jak by měl z hlediska návrhu fungovat. Poslední část se zmiňuje o uživatelském rozhraní, kde se detailně popisují jednotlivé komponenty GUI.

Stěžejní kapitolou je pátá, která nese název Implementace. Detailně informuje o implementaci jednotlivých fází. Veškeré problémy jsou detailně zpracovány a vysvětleny jejich řešení. Nejdříve se zmiňuje o implementaci skenování sítí. Pokračuje se nastavením a podrobným popisem algoritmu pro výpočet nejvhodnějšího kanálu. Hlavní částí této kapitoly je popis vytváření testů.

Sedmá kapitola popisuje souhrn a testování vytvořeného nástroje. Zmiňuje se o fázích testování a informuje o zařízeních, které byly potřebné pro provádění testů. Navíc uvádí příklady dvou typů testování na sítích s různým šifrováním. V závěru shrnuje veškerou práci na testech a nástroji.

Další možnosti rozšíření, je název osmé kapitoly, která nemůže chybět. Zmiňuje se o možných dalších rozšířeních, které by mohli po dokončení práce pokračovat ve vývoji.

A poslední devátou kapitolou je závěr, který shrnuje veškeré výsledky nástroje a odvozuje z nich celkové hodnocení práce.

Kapitola 2

Wi-Fi jako standard

V roce 1997 vytvořila organizace IEEE (Institute of Electrical and Electronic Engineers) standard s označením IEEE 802.11. Tento standard popisuje bezdrátové sítě (tzv. WLAN) neboli Wi-Fi. Nejedná se o žádnou zkratku typu Wireless-Fidelity (Bezdrátová věrnost), jak se někteří domnívají [1]. Jde o čistě marketingový název pro standard IEEE 802.11. Informace v této kapitole jsou čerpány z knihy Wi-Fi Security [2].

2.1 Základní informace o WiFi sítích

Bezdrátové sítě se z geografického hlediska dělí do dvou základních kategorií.

1. **Ad-Hoc sítě**

   Tato síť se vyznačuje minimálně dvěma stanicemi v blízkém dosahu. Komunikace probíhá přímo a bez prostředníka. Vhodná je např. do menších prostor, kde se všechny stanice musí pokrýt signálem. Nastavení takové sítě je náročné a používá se spíše při spojení několika stanic pro sdílení složek či hraní her. Další nevýhodou je nízká úroveň zabezpečení.

2. **Infrastrukturní sítě**

   Síť, která je tvořena přístupovým bodem, tzv. access-pointem (zkráceně AP). Tento přístupový bod vymezuje infrastrukturu pokrytí signálem, kde je možné se připojit. Výhod má tato síť mnoho. Například možnost centrální správy a díky tomu i kvalitnější zabezpečení. Jednodušší konfigurace a možnost propojení i více AP a tím zvýšení pokrytí signálem, čímž se zvýší limit maximálně připojených uživatelů. Za nevýhodu může být považována právě nutnost access-pointu.

Infrastrukturní síť je tvořena klientskými stanicemi, které se připojují k přístupovému bodu pomocí svých síťových Wi-Fi karet. Každá Wi-Fi síť má jednoznačný identifikátor daný administrátorem sítě. Jde o SSID (Service Set Identifier), odesílá se pomocí beacon frame (majákového rámce), pravidelně několikrát za vteřinu. Zde jsou obsaženy informace o dané bezdrátové síti.

2.2 Princip přenosu dat na fyzické vrstvě

- **DSSS (Direct Sequence Spread Spectrum)** Metoda přímo rozprostřeného spektra. Principem je vygenerování většinou pseudonáhodné dvojkové posloupnosti čísel

(tzv. Chipů), pomocí např. Barkerova kódu. Na tento kód se rozprostřou jednotlivé bity určené k odeslání, čímž vznikne nadbytečnost.

Princip: nedochází k přenosu určitého bitu, ale skupiny bitů, kterým se říká chip neboli úlomek. Při odeslání bitu s hodnotou log. 1 dochází k odeslání chipu a při odeslání bitu s hodnotou log. 0 dojde k odeslání invertovaného (invertované skupiny bitů). Díky tomu je přenášený signál více odolný vůči zarušení, protože je rozprostřen do většího rádiového spektra.

- **OFDM (Orthogonal Frequency Division Multiplexing)** Jedná se o Ortogonální Frekvenčně Dělený Multiplex. Princip spočívá v namapování bitů na několik stovek až tisíců nosných frekvencí. Nosné frekvence jsou dále modulovány pomocí některé z robustních modulací, např. QPSK, 16-QAM či 64-QAM. Díky velmi malým datovým tokům na jednotlivých tocích lze vkládat ochranné intervaly z důvodu jednoznačného odlišení přijímaných dat. Tato metoda je vcelku pomalá, ovšem po sečtení všech kanálů se maximální teoretická rychlost vyšplhá na 54 Mbit/s.
- **FHSS (Frequency hopping spread spectrum)** Metoda "rozprostřeného spektra s přeskakováním kmitočtů". Základním principem je vysílání krátkých datových toků na určité frekvenci, kdy se po uplynutí časového limitu mění pseudonáhodně vysílací frekvence. Jedná se o periodickou sekvenci skoků, kterou zná pouze vysílací a přijímací strana.
- **DFIR (Diffused Infrared)** Přenos přes infračervené záření, které má ale mnoho nevýhod, např. paprsek se snadno odráží a neprochází pevným materiálem. Problémem je i finančně náročnější realizace. V praxi se tudíž tolik nepoužívá.

2.3 Princip přenosu dat na linkové vrstvě

Princip přenosu na linkové vrstvě se u 802.11 skládá ze dvou podvrstev. První z nich je LLC a druhá MAC

- **LLC (Logical Link Control)** Tato vrstva je prostředníkem mezi MAC a síťovou podvrstvou. Zajišťuje přenos datových rámců na WLAN (mimo jiné).
- **MAC(Media Access Control)** V rodině protokolu 802.11 se používá MAC přístupová metoda, známá jako:

CSMA / CA (Carrier Sense Multiple Access / Collision Avoidance)

Jedná se o metodu s vícenásobným přístupem, s naslouchánim na sdíleném médiu. Přívlastek CA jí odlišuje od přístupové metody CSMA/CD, která je známá z klasického ethernetu. U 802.3(ethernet) dochází k detekci kolize, tzn. že se sleduje, zda na síti nedošlo ke kolizi. Pokud ano, vyšle se tzv. JAM signál na všechny síťové karty. Ty si vygenerují náhodné číslo a začne odpočet. Ta stanice, které skončí odpočet jako první, může začít vysílat. U 802.11 nic takového není. Tato metoda pracuje pouze v poloduplexním režimu, takže detekce kolize zde není možná. Principem je naslouchání po určitou dobu, zda-li je přenosové pásmo volné. Pokud není provoz na síti, stanice si zažádá o vysílací pásmo a teprve poté, co ho dostane, začne vysílat. Po odeslání čeká na potvrzení od příjemce, zda zpráva došla bez problému. Pokud ne, snaží se o opětovné odeslání.

2.4 Přehled nejznámějších standardů IEEE 802.11

Výpis nejznámějších standardů IEEE 802.11 [3].

- **IEEE 802.11** Jedná se o původní standard s přenosovou rychlostí 1-2Mbit/s a frekvencí 2,4GHz z roku 1999.
- **IEEE 802.11a** Tento standard vznikl v roce 1999. Pracuje na frekvenci 5GHz a to se dá pokládat za výhodu, protože většina bezdrátových zařízení pracuje na frekvenci 2,4GHz (Mikrovlnné trouby, Bluetooth, většina Wi-Fi sítí, atp.), což způsobuje větší zarušení. Celkově je tento standard více propracovaný než 802.11b a 802.11g. Je zde povolen vyšší maximální vyzařovací výkon a to může být vhodné při propojení na delší vzdálenosti. K modulaci využívá OFDM a dosahuje maximální teoretické rychlosti 54Mbit/s.
- **IEEE 802.11b** Vznikl také v roce 1999 a je to nástupce IEEE 802.11. Pracuje na frekvenci 2,4GHz a došlo zde k nárůstu maximální teoretické rychlosti na 11Mbit/s. Vysílá se na několika vyhrazených kanálech. Pro komunikaci na fyzické vrstvě využívá modulaci DSSS.
- **IEEE 802.11g** Vznikl v roce 2003. Navazuje na standard 802.11b a je s ním zpětně kompatibilní. Dosahuje maximální teoretické rychlosti 54Mbit/s a to z důvodu použití OFDM. Aby byl zpětně kompatibilní, tak podporuje i DSSS. Pracuje na stejné frekvenci 2,4GHz a používá stejné kanály.
- **IEEE 802.11n** Na tomto standardu se začalo pracovat již v roce 2003 a oficiální schválení padlo až v roce 2009. Cílem bylo zvýšit přenosovou rychlost a vyrovnat se alespoň 100Mbit/s, jakou známe z Ethernetu 100base-TX. Základní změnou je úprava MAC podvrstvy a fyzické vrstvy. Díky tomu je teoretická rychlost neuvěřitelných 600Mbit/s. Protože ale 802.11 pracuje v poloduplexním režimu, tak lze teoreticky dosáhnout jen 300Mbit/s při použití 40MHz šířky pásma. Ale pouze teoreticky.

Teoretická vs Reálná rychlost přenosu

Tabulka 2.1 ilustruje rozdílné hodnoty při teoretických a reálných rychlostech, kterých lze na různých verzích standardu IEEE 802.11 dosáhnout.

Verze	Teoretická rychlost	Reálná rychlost
802.11b	10 Mbit/s	5 Mbit/s
802.11g	54 Mbit/s	20 Mbit/s
802.11n	300 Mbit/s	130 Mbit/s

Tabulka 2.1: Porovnání teoretických a reálných přenosových rychlostí.

Proč dochází k takovému poklesu lze jednoduše vysvětlit. Jednotlivé operace na MAC vrstvě, které slouží ke spolehlivému odeslání a kontrole, sníží rychlost o 30 až 40%. Další snížení dochází při komunikaci protože, jak jsem se již zmiňoval, standard 802.11 komunikuje v poloduplexním režimu. Další ztráty vznikají vlivem okolí, což v naprosto ideálních podmínkách nelze nikdy dosáhnout. V následující kapitole se podrobně analyzují problémy, které jsou s bezdrátovými sítěmi spojeny.

Kapitola 3

Analýza problémů

Vyšší bezpečnostní opatření u bezdrátových sítí je daň, která se musí platit za odproštění od klasického ethernetu. Zabezpečení je jedna z hlavních nevýhod bezdrátových technologií. Bez důkladného zabezpečení je síť nebezpečným prostředkem pro útočníka. Může jít o běžného uživatele, který se snaží pouze dostat skrze Wi-Fi síť do sítě internet, ale může se jednat i o cílený útok, který má za cíl odcizit, využít či znehodnotit důležitá nebo důvěrná data. Následující kapitola se podrobněji zabývá bezpečnostní analýzou, vyhodnocením bezpečnostních rizik a doporučením, které mají zvýšit úroveň zabezpečení.

Mezi základní bezpečnostní funkce patří:

- **Diskrétnost** - Při diskrétnosti jde o snahu uchovat informaci v rámci jedné sítě, aby se dále nešířila. Diskrétnost se dá dodržet například šifrováním důvěrných dat.
- **Integrita** - Integrita je velmi důležitá část bezpečnosti. Jde o záruku, že doručený paket nebyl cestou nijak pozměněn, či nebyl odeslán z jiného zdroje než je předpokládáno.

Následující část kapitoly se zabývá bezpečnostními problémy. V každé části je navíc zmínka o vhodném řešení, nebo popřípadně jakým nástrojem se bezpečnostní slabina dá odhalit. Nejčastěji zmiňovaný nástroj se nazývá *Aircrack-ng* [4], který v sobě zahrnuje mnoho dalších jako jsou *Aireplay-ng*, *Airodump-ng*, *Airmon-ng*, ...

Vyzařovací výkon Wi-Fi sítě

Nejlepší ochranou před útokem na Wi-Fi síť je eliminování rozsahu, odkud lze daný útok provést. S klesající úrovní signálu se přímo úměrně zvyšuje doba, potřebná pro její úspěšné prolomení. Omezením vysílacího výkonu na hodnotu nezbytně nutnou (v rámci budovy, areálu atp.) se zvyšuje úroveň zabezpečení. Zbytečně se tak nezarušuje frekvenční pásmo v místech, kde se již k dané síti nepřipojují žádní klienti a zároveň dává prostor pro jiné Wi-Fi sítě, které využívají stejný kanál.

SSID

Jak jsem se již zmínil, SSID se odesílá jako identifikátor ve formě beacon rámců, které zachytí každá klientská stanice v dosahu signálu. Zapnuté SSID neznamená hned bezpečnostní riziko, ale silně se doporučuje změnit si defaultně nastavené SSID od výrobce. Síť, která má takové SSID ponechané, má mnohem větší pravděpodobnost, že se nějaký útočník bude snažit do ní dostat. Důvodem je domněnka, že taková síť patří uživateli, který

nerozumí bezpečnosti Wi-Fi sítí. Ponechané SSID a heslo z továrního nastavení výrobce je velmi nebezpečné a lehce prolomitelné [5].

Na druhou stranu, zakázané vysílání SSID se nesmí brát jako dostatečné zabezpečení. Jedná se o tzv. falešný pocit bezpečí, protože si administrátor může myslet, že pokud jeho síť nelze vyhledat, nikdo jiný se k ní nepřipojí. Útočníkovi stačí odposlouchávat provoz na síti, jelikož se při přijení klienta k access-pointu se zakázaným SSID, tento název posílá po síti v otevřené formě.

Zjištění SSID se dá provést například nástrojem *Aireplay-ng*. Ten odposlouchává provoz na síti a po odposlechnutí potřebných paketů zobrazí název SSID.

3.1 WEP šifrování

Anglická zkratka „Wired Equivalent Privacy“ znamená zabezpečení, které je ekvivalentní drátovým sítím. Pro šifrování se využívá algoritmu RC4. Pro kontrolu správnosti přenesených dat se využívá 32 bitový kontrolní součet. WEP se nejčastěji využívá buď jako 64 bitové, nebo 128 bitové. Oba typy obsahují prvních 24 bitů inicializační vektor, což znamená, že na 64 bitový WEP se využívá 40 bitového klíče a na 128 bitový WEP klíč dlouhý 104 bitů. Tento šifrovací standard je v dnešní době (rok 2011) zastaralý, bezpečnostně velmi slabý a nedoporučuje se používat. Pokud se jedná o starší zařízení, podporující pouze šifrování WEP, doporučuje se využívat více bezpečnostních prvků (Zakázání SSID, filtrování MAC adres, atd.) [6].

Známé typy útoků na Wi-Fi síť zabezpečenou šifrováním WEP

- **DoS útok** - Na přístupový bod je odesláno velké množství paketů, které nezvládne zpracovat. Klienti tím přijdou o přístup do sítě.
- **FMS útok** - Objevil se v aplikaci *AirSnort* v roce 2001 [7]. Základní podmínkou úspěchu je odposlechnutí obrovského množství paketů. Bylo zapotřebí najít tzv. „slabý“ paket s unikátním inicializačním vektorem, který byl pro cracknutí klíče nezbytný. Tudíž pro úspěšný útok bylo zapotřebí velikého úsilí.
- **Korek útok** - V roce 2004 hacker jménem KoreK prolomil WEP šifrování na základě statistické kryptoanalýzy. Již nebylo zapotřebí slabých paketů, jak tomu bylo u FMS. Principem je odposlechnutí velkého množství paketů se stejným inicializačním vektorem. Tento typ útoku je v modifikované formě použit také v nástroji jako PTW. Útok lze provést pomocí nástroje *Aircrack-ng*.
- **Derivace klíče pomocí CRC-32** - Využívá se slabého místa kontrolního součtu (CRC). Dojde k odchycení paketu, v něm se data změní tak, aby CRC souhlasilo a odešle se na přístupový bod. Ten, protože CRC souhlasí, předá paket na vyšší vrstvu OSI modelu, ve které dojde k odeslání ICMP zprávy s chybovým hlášením. Tím lze odhadnout klíč pro daný inicializační vektor. Nástroj, obsahující tento typ útoku je například *AirSnort*. Jeho vývoj ale již zkončil, proto lze opět využít nástroje *Aircrack-ng*.
- **Induktivní derivace klíče** - Princip je závislý na přidělení veřejných IP adres pro klientské zařízení. Pokud se přes internet budou odesílat stejná data na klientské

stanice, lze tento provoz odchytit a pokusit se o derivaci klíče. Jelikož se šifrují stejná data stejným klíčem, tak existuje omezený počet podob zašifrované zprávy, než se začne inicializační vektor opět opakovat.

- **Caffé Latté** - Další typ útoku, jak zjistit klíč u zabezpečení WEP. Nejedná se o klasickou metodu sniffování paketů, ale zjišťuje heslo přímo od klientské stanice na základně známých nevýhod. Tento typ útoku byl vymyšlen pro využití hlavně v internetových kavárnách a nalezení hesla by nemělo trvat déle, než si útočník vypije svoje Caffé Latté. Principem je rozesílání falešných ARP dotazů. Na rozdíl od předchozích útoků, které používají pro zjištění hesla AP, tento ho zjišťuje od připojených klientů. Nástroj, obsahující Caffé Latté útok je *Aircrack-ng*.

3.2 WPA šifrování

„Wi-Fi Protected Acces“, neboli Wi-Fi s chráněným přístupem. Vznikl na reakci vážných nedostatků, které mělo šifrování WEP. Vychází z návrhu standardu 802.11i. Aby nebyl pro výrobce problém s výměnou HW, tak se i u WPA využívá algoritmus RC4, stejně jako u WEP, čímž stačilo pouze upravit software access-pointů, bezdrátových karet a dalších zařízení na nové zabezpečení. WPA využívá inicializační vektor dlouhý 48bitů a šifrovací klíč délky 128 bitů. Také se jedná o zastaralé zabezpečení, které se pokud možno nedoporučuje, i když prolomení je obtížnější než u šifrování WEP.

WPA TKIP

"Temporal Key Integrity Protokol", který je definován dle specifikace IEEE 802.11i. Byl navržen pro zvýšení bezpečnosti šifrování bez nutnosti měnit hardware a využít stejný šifrovací algoritmus RC4 jako je tomu u WEP. Prvním vylepšením je použití delšího šifrovacího klíče, který je u této specifikace 128 bitů. Hlavním rysem TKIP je, že pro každý paket se mění klíč, podle kterého se šifruje. Klíč se vytváří mícháním různých kombinací jakou jsou číslo klíče, číslo paketu, MAC adresa, ...

Prolomení WPA s kombinací s protokolem TKIP se již podařilo a na začátku roku 2009 bez větších nároků na vybavení za čtvrt hodiny [8]. Na začátku roku 2011 již není problém TKIP prolomit do jedné minuty, což z ní činí také nedokonalé zabezpečení.

WPA AES

AES byl vyvinut z důvodu nedostatečně bezpečnému šifrovacímu standardu DES, který se podařilo prolomit. V kombinaci s CCMP protokolem se jedná o velmi silnou formu zabezpečení, která příliš nezatěžuje výkon při šifrování. Označuje se také jako symetrická bloková šifra, která šifruje data s pevnou velikostí 128 bitů. V dnešní době patří mezi nejlepší volbu při výběru šifrování, díky jeho statusu neprolomitelnosti.

U zabezpečení WPA s protokolem AES nelze prolomit stejným způsobem jako tomu je u TKIP. Aktuálně se to žádnému útoku nepovedlo. Jedná se o silně doporučované a dosti bezpečné šifrování [9].

WPA 2 TKIP / AES

WPA2 je označován za jednu z nejlepších variant, jak ochránit bezdrátovou síť. Z bezpečnostního hlediska se při použití WPA2-TKIP před WPA-TKIP nejedná o žádnou bezpečnostní výhodu. Již je také známý útok, při němž došlo k prolomení WPA2-TKIP [10].

Stejně jako není bezpečnostní rozdíl u protokolu TKIP u WPA a WPA2, tak tomu není ani u AES jinak. Každopádně se jedná o doposud neprolomené zabezpečení, které se dá považovat za dostatečně silné.

Zranitelnost WPA 2

I WPA 2 má zranitelná místa, která by měl kvalitní administrátor sítě znát [11]. S kombinací s PSK je zabezpečení náchylné k odposlechu a k slovníkovému útoku, což lze dokázat nástrojem *Aircrack-ng*. Dále zranitelnost při použití certifikátu pomocí PEAP, kdy lze donutit protokol, aby ignoroval certifikát. Další možností je odhadnutí adresy podsítě při použití WPA 2 s kombinací s TKIP, což může při drobném upravení rámců způsobit narušení sítě.

WPA - Personal mode

Běžný způsob zabezpečení bezdrátové sítě. V tomto režimu se používá jako heslo buď PSK, nebo přístupové heslo. PSK je poté dynamicky posílán mezi AP a klientem.

WPA - Enterprise mode

V enterprise módu se používají veškeré funkce z Personal módu + podpora 802.1x a Radius serveru pokud je nasazen jako autentizační server. Pokud se využívá k připojení Personal mód, je potřeba aby byli všichni klienti zaregistrovány na access-pointu. Pokud se využije Enterprise-mód, používá se centrální databáze na 802.1x Radius serveru.

Radius server

Patří do vysoké úrovně zabezpečení přístupu k síti. Provádí se pomocí autentizace uživatele. Network Access Server, neboli Radius klient vyšle dotaz na autentizaci přes PPP (Point-to-Point Protocol) protokol. Uživatel vyplní údaje, a Radius klient odešle zašifrované informace na Radius server. Ten ověří autentizační údaje a odpoví povolením přístupu, nebo zamítnutím.

Porovnání zabezpečení

Typ	Autentikace	Šifrování	Firemní sítě	Malé sítě
WEP	není	WEP	velmi slabé	slabé
WPA (PSK)	PSK	TKIP	slabé	dobré
WPA 2 (PSK)	PSK	AES-CCMP	slabé	výborné
WPA	802.1x	TKIP	dobré	výborné (drahé)
WPA 2	802.1x	AES-CCMP	výborné	výborné (drahé)

Tabulka 3.1: Porovnání zabezpečení.

Tabulka 3.1 porovnává jednotlivé typy šifrování v kombinaci s autentikací a jejich bezpečnostní úroveň při nasazení ve firemních nebo malých/domácích sítí.

Filtrování MAC adres

Další zajímavé zabezpečení nejen u sítí typu 802.11 je filtrování dle MAC adres. Jedná se o nízkoúrovňové filtrování hardwarových adres. Používají se dva typy filtrů:

1. **Blokování stanic podle MAC adres uvedených v seznamu**

   Seznam pouze obsahuje výčet blokovaných MAC adres. Pokud se připojí klient s MAC, která se shoduje s adresou ze seznamu, dojde k zablokování (Seznam se také označuje anglickým výrazem black-list). Slabé řešení, které se v praxi příliš nenasazuje.

2. **Povolení komunikace stanic podle MAC adres uvedených v seznamu**

   Jedná se o silnější řešení než blokování MAC adres. Pro úspěšné prolomení je potřeba zjistit MAC adresu připojeného klienta. Při použití tohoto typu zabezpečení, se musí udržovat stále aktuální seznam MAC adres. Stejně tak by se měl před zavedením administrátor zamyslet, na jakých portech tento bezpečnostní prvek implementovat, aby nedocházelo ke zbytečnému zatěžování firewallu. U větších sítí se tento princip příliš nevyužívá.

Vypnutí DHCP serveru

Jedna z možností, která by mohla zvýšit bezpečnost, je vypnutí DHCP serveru a nastavení statického rozsahu povolených IP adres. Uživatel se sice připojí, ale pokud nezná rozsah IP adres, které jsou povolené, nemůže využít komunikaci po síti. Pro zjištění správného rozsahu ovšem stačí odposlouchávat broadcast pakety na síti. Nejedná se tudíž o velké bezpečnostní opatření, ale v kombinaci s ostatními bezpečnostními prvky jde o dobrou volbu.

Autentizace přes webové rozhraní

Zneužití autentizace přes webové rozhraní je útok spíše ojedinělý, ale patří mezi možnosti, jak se dostat do sítě. Pokud se pro přihlášení do sítě používá pouze autentizace přes webové rozhraní, je to příležitost i pro šikovného útočníka. Pro zjištění hesla to znamená vynaložení většího úsilí než u ostatních útoků. Osoba, která se chce neoprávněně dostat do sítě, si potřebuje vytvořit podobnou přihlašovací stránku, jako je ta reálná. Nastaví se stanice, aby se tvářila jako Access Point, nastaví stejné SSID na stejném kanálu. Pro vyrušení sítě musí využít antény s vyšším ziskem. Tím pádem stačí, aby se uživatel sítě chtěl připojit a zadal identifikační údaje, které se odešlou útočníkovi např. na email a bezpečnost je prolomena.

MAC Poisoning

Pokud neprovozuje AP zašifrovanou komunikaci a filtruje pouze MAC adresy dle pravidel firewallu, tak lze odposlechnout příslušný paket, který obsahuje MAC adresu autorizované stanice. Poté stačí počkat, než se klient odpojí (nebo ho odpojit násilně) a vydávat se za něj s jeho MAC adresou.

Brute-force

Prolomení ochrany hrubou silou, která se provádí zkoušením různých kombinací číslic a písmen, nebo slovníkovým útokem. Slovníkový útok je rychlejší a efektivnější u jednoduchých hesel. Nejvýraznější novinkou u *brute-force* útoku je využití grafického procesoru nVidia. Výhodou je vyšší rychlost generování kombinací a nezatěžování samotného CPU. Samotný brute-force útok, který zkouší veškeré kombinace písmen, je velmi náročný a u složitějších hesel téměř nepoužitelný. Zároveň se jedná o jedinou možnost jak prolomit zabezpečení WPA / TKIP v nástroji WST. Nelze využít chyby jako u šifrování WEP. Proto je zde velmi důležité jak silné heslo se nastaví. Může se používat nejsilnější šifrování, ale s kombinací se slabým heslem je to naprosto zbytečné.

Tento typ útoku lze využít použitím nástroje *Aircrack-ng*. Další možnost, jak provést slovníkový útok, je například pomocí konzolové linux aplikace *Cowpatty*. Oba nástroje využívají k útoku hesla ze slovníku.

ARP Poisoning

Otrávení ARP tabulky se provádí jejím naplněním podvrženými údaji. Poté co se chce klient připojený k access-pointu např. podívat na určitou internetovu stránku, pošle stanice ARP dotaz a vrátí se „otrávená odpověď“. Jedna z možností jak provést útok *man-in-the-middle*. Na otrávení ARP tabulky lze použít program *ettercap*.

Packet injection

Technika injekce paketů pracuje se softwarovou úpravou části, či celého paketu (např. změna hlavičky, změna dat, jiné části). Tento útok má za cíl přesměrovat provoz u takových sítí, kde nelze použít *ARP Poisoning*. Některé ovladače bezdrátových síťových karet nedovolují použití injekce paketů, proto je potřeba použít jiné, které nemají podobné ochrany. Nástroj pro injekci paketů se jmenuje *Aireplay-ng*.

3.3 Existující testovací nástroje

Backtrack

Upravená distribuce, která vychází z Ubuntu. Nástroj je implementován konkrétně ve verzi BackTrack 5, která vychází z Ubuntu 10.04 „Lucid Lynx“. Obsahuje spoustu nástrojů, které se dají využít na crackování sítí. Mimo jiné například *Aircrack-ng*, o kterém je zmíňka v následujícím odstavci. Obsahuje upravené ovladače pro snadné sniffování, monitorování a injekci paketů. Distribuce je prezentována jako live s možností nainstalování na disk či flash disk. Samotná live verze je upravená na nezbytně nutné minimum programů, které jsou potřeba při práci s ním. Naopak ale obsahuje navíc velké množství nástrojů, které byste jen těžko hledali v jiné distribuci. Od crackovacích nástrojů přes brute-force nástroje až po aplikace na provádění reverzního inženýrství. Po instalaci se dá používat i jako normální systém a umožňuje doinstalovat jakýkoliv program, který pracuje pod linuxovou distribucí Ubuntu.

Aircrack-ng

Na manuálových stránkách popsán jako „a 802.11 WEP / WPA-PSK key cracker“, který má pod sebou dalších osmnáct nástrojů pro práci s bezdrátovou sítí. Obsahuje také nespočet útoků, skenovacích utilit,... Velmi známý a oblíbený nástroj jak mezi administrátory sítí, tak mezi crackery. Mnoho zaniknutých nástrojů, které prováděly specializované útoky, se sdružily právě do aplikace *Aircrack-ng*. Mezi nejznámější patří mimo *Aircracku-ng* například *Airmon-ng*, který se stará o přepnutí bezdrátového rozhraní do monitor módu. Nástroj *Airodump-ng* zachytává provoz pomocí monitor módu v dosahu bezdrátové karty a vypisuje jej do přehledné tabulky přímo v konzoli. Zároveň podporuje zachytávání IV nebo WPA handshake. Další vemi známý nástroj je *Aireplay-ng*, protože zvládá injekci paketů do nejrůznějších typů útoků.

Kapitola 4

Návrh řešení

Kapitola seznamuje se základními požadavky a návrhy při vytváření nástroje. Nejdříve informuje o požadavcích aplikace, dále o principu, jak by měl nástroj vypadat a nakonec se zmiňuje o uživatelském rozhraní.

4.1 Požadavky aplikace

Hlavní požadavky při vytváření nástroje shrnuty do hlavních bodů.

- **Přenositelnost** - V návrhu se hned uvažovalo o zaručené přenositelnosti díky zakomponování nástroje do Live linuxové distribuce. Jedná se o upravenou distribuci BackTrack [12], která v sobě již obsahuje veškeré další potřebné nástroje. Obsahuje také upravené ovladače bezdrátových síťových karet, které podporují potřebné operace jako jsou monitor mód, či injekce paketů.
- **Jednoduché a přehledné ovládání** - Ne každý administrátor sítě rád pracuje s terminálem, nebo s příkazovým řádkem. Proto se od návrhu počítalo s jednoduchým a přehledným ovládáním, které by mělo být jasné na první pohled, aniž by předtím s nástrojem pracoval.
- **Možnosti nastavení širšího rozsahu testování** - Možnost zvolit si více testů, které se provedou za sebou. Daná síť se tak otestuje komplexněji a je možnost najít více bezpečnostních děr. Uživateli ušetří takové testování mnoho času, protože se testy provádějí automaticky po sobě.
- **Vyhodnocení úrovně zabezpečení** - Po dokončení testů zobrazit souhrnné informace o testech. Vypsat výsledky, důležité informace a doporučení, které by vedli ke zvýšení úrovně zabezpečení.

Hlavním požadavkem nástroje bylo vytvořit jednoduché, přehledné a lehce ovladatelné rozhraní pro testování úrovně zabezpečení Wi-Fi sítí. Aplikací by mělo být možné testovat různými typy útoků odolnost vybrané Wi-Fi sítě. Aplikaci jsem nazval *WST*, což je zkratka pro "Wi-Fi Security Tool". Uživatel by měl být schopen bez problémů zvládnout ovládání programu a to i s nízkou odbornou znalostí problematiky zabezpečení sítí.

4.2 Princip funkce

Po spuštění aplikace se uživateli zobrazí grafické rozhraní. V prvním kroku si uživatel naskenuje dostupné Wi-Fi sítě. Může si vybrat různé testy na zvolenou síť, kterou si lze vybrat ze seznamu pokročilého nastavení. Na výběr je i volba na zjištění skrytých sítí, které mají zakázané vysílání SSID. Úroveň testování bude možno vybrat ze dvou typů. V prvním základním typu se nachází posuvník, kterým se vybere jaké množství testů, tudíž jak důkladně se má daná síť otestovat. V druhém pokročilém typu si bude moci uživatel zvolit jednotlivé testování sám. Po spuštění testování se začnou jednotlivé útoky provádět na danou síť a průběžné výsledky, včetně důležitých informací se budou zobrazovat v informačním okně. Po ukončení testování se zobrazí okno se souhrnnými informacemi a doporučeními.

4.3 Uživatelské rozhraní

Návrh je vytvořen v GUI Qt pro jazyk C++ [13]. Skládá se z několika základních částí.

- **Skenování** - V návrhu se uvažovalo s možností vybrat si rychlé skenování Wi-Fi sítí, které mají aktivní vysílání SSID, nebo odposlouchávání a zjištění názvu skrytých sítí. Mimo jiné se v okně objeví i základní informace o sítích.
- **Nastavení** - Nastavení jsem rozdělil na 2 základní části a to na základní a pokročilé. V základním si uživatel zvolí úroveň testování. To se bude dělit na několik částí a čím více se bude posuvník pohybovat k hodnotě MAX, tím budou testy náročnější. V pokročilém nastavení si bude moci přímo uživatel nastavit jaké útoky na danou síť hodlá použít.
- **Informační okno** - Průběžně bude zobrazovat informace o testování a o právě prováděné operaci. Celkový výsledek se zobrazí ve zvláštním okně, který bude statistickým souhrnem vybraného útoku s výsledkem, na jaké úrovni se zabezpečení nachází. Test bude možné kdykoliv ukončit a uzavřít aplikaci.

Po dokončení návrhů, se postupně začalo s realizací a přišlo se na celou řadu problémů. Posléze došlo k drobným úpravám a přidání nových funkcí. O tom všem je následující kapitola která se zabývá implementací nástroje.

Kapitola 5

Implementace

Samotná implementace probíhala v několika fázích. Nejdříve byla zaměřena na vytvoření uživatelského rozhraní, které bylo v průběhu tvorby několikrát částečně upraveno. V další fázi se implementace zaměřila na skenování Wi-Fi sítí v dosahu. Ta byla rozšířena na další části, které jsou popsané v následující kapitole. Poté došlo k implementaci ostatních oken jako jsou například nastavení, či informace o programu. V poslední části se jedná již o samotnou implementaci testů včetně finálního výpisu po ukončení testů.

Během implementace jsem využíval verzovací systém Git, pro správu a zálohu celé bakalářské práce, včetně všech zdrojových souborů. Na serveru je nastaveno kopírování na další dva disky pro vysokou úroveň zálohy.

5.1 Skenování Wi-Fi sítí

Při skenování sítí, které jsou v dosahu, se rozděluje program na tři základní části. Každá část je popsaná zvlášť.

1. **Jednoduché skenování**

   Již od návrhu se počítalo využít pro skenování Wi-Fi sítí nástroj *iwlist*, který je standardní součástí linuxových distribucí. Ještě před začátkem práce s tímto nástrojem bylo potřeba zjistit bezdrátové rozhraní, na kterém se má skenování okolních sítí provést. K tomu byla využita funkce *iwconfig*, ze které se vyparsují bezdrátová rozhraní podporující standard IEEE 802.11. Tyto rozhraní jsou uložena do dynamického pole řetězců. Po spuštění je zvoleno základní rozhraní jako první ze seznamu. V nastavení lze změnit rozhraní buď z rozbalovacího seznamu, který obsahuje uložená rozhraní, nebo možnost ručně zadat název, či IP adresu např. při použití externí sondy. Výstup nástroje *iwlist* je také vyparsován a uložen do vektoru struktur. S tímto vektorem se dále pracuje při výpisu sítí do tabulky a při spuštění samotného testování, protože obsahuje veškeré informace o sítích.

2. **Interaktivní režim skenování**

   Jak již nadpis naznačuje, v této části se interaktivně v seznamu mění jak sítě, tak informace o nich (síla signálu atp.) . S tímto se v návrhu původně nepočítalo. Jedná se o vylepšení, které zvyšuje komfort při ovládání. Uživatel může mít aktivní tento režim a pohybovat se po prostorech, se zobrazením kde všude má signál a kde je nejlepší místo k provádění testů.

Z návrhu se původně uvažovalo o použití nástroje *tcpdump*, který zachytává veškeré beacon rámce a vypisuje na standardní výstup. Zde ovšem nastal problém s přesným parsováním výsledků. Nejdříve by se musel zvolit interval, po jakém zpracovat výstup z nástroje. *Tcpdump* je volán pomocí funkce *popen* a výstup se zapisuje po určitém počtu znaků do řetězce, tudíž se nejedná o celé řádky. Takže první problém by nastal při přesném ořezání a tudíž např. neúmyslným zahozením nějakého beacon rámce, který by pak zkresloval výsledky. Dalším problémem by byl výpočet síly signálu pro každý paket zvlášť (při vysokém počtu beaconů za sekundu příliš náročné). Navíc by bylo potřeba ukládat informace o příchozích beaconech a vypočítávat z nich průměrné hodnoty signálu. Také porovnávat příchozí pakety s existujícími sítěmi ze seznamu, jestli již nevypršel maximální beacon interval, po kterém lze vyřadit síť ze seznamu. Z těchto důvodů jsem se rozhodl hledat jiné řešení, které by bylo jednodušší a tím pádem méně náročné jak na realizaci tak na samotný chod.

Další možností bylo využít opět nástroje *iwlist*, jako v případě jednoduchého skenování. Ovšem spouštět tento nástroj v krátkých pravidelných intervalech by nebylo zrovna nejvhodnější řešení. Navíc pokud se tento nástroj spouští vícekrát po sobě, přestane vracet naskenované sítě a začne vypisovat chybová hlášení.

Jako nejvhodnější řešení se ukázalo využití nástroje *Airodump-ng*, který patří do balíčku *Aircrack-ng*. Při vybrání vhodných přepínačů, které lze vybrat po nastudování manuálových stránek, není problém vypisovat v pravidelném intervalu potřebné informace a poté je vcelku jednoduše zpracovat. Veškeré potřebné operace, jako výpočet signálu, či odebírání a přidávání sítí v závislosti na přijatých beacon rámcích, již dělá nástroj *Airodump-ng* sám. Tím se celý proces velmi zjednodušuje.

Poslední problém nastal při zpracování dat v pravidelném intervalu. Bylo potřeba rozdělit řízení, aby nedocházelo k zamrzání GUI a zároveň se provádělo pravidelné zpracování dat a jejich výpis na GUI. K tomuto účelu jsem využil rozdělení na více procesů. Zde se ovšem vyskytl další problém. Synovský proces totiž nemůže zapisovat do GUI, a navíc má syn a otec oddělený paměťový prostor. Proto bylo rozhodnuto vytvořit sdílenou paměť a pomocí mezi-procesové komunikace (IPC) využít signály, které kontaktují otcovský proces, aby vypsal data ze sdílené paměti do tabulky. Opět to ale znamenalo v pravidelných intervalech zapisovat do sdílené paměti, číst a mezitím neustále vysílat signály.

Nakonec jsem tento problém vyřešil pomocí funkce QThread [14], čímž se vytvoří druhé vlákno, které již nemá oddělený paměťový prostor, jak je tomu právě u více procesů. Tím se odstranil problém zápisu do sdílené paměti a vysílání signálů. Celý problém se tak elegantně a jednoduše vyřešil.

3. **Skenování sítí se skrytým SSID**

   Využitím nástroje *Aireplay-ng* se zachytává provoz na síti. V případě připojení klienta do sítě se zobrazí skryté SSID, čímž lze danou síť označit a určit pro testování.

4. **Ruční zadání SSID**

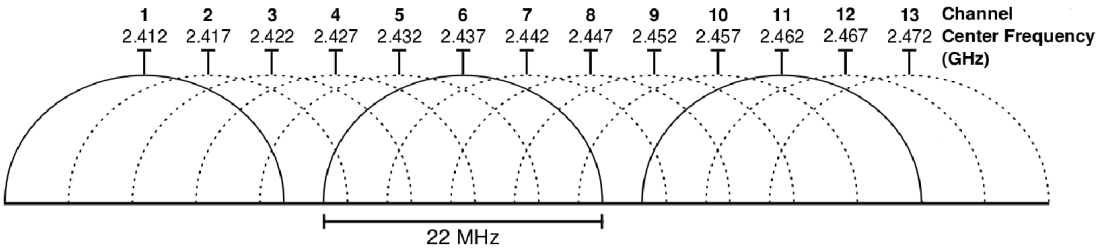
   V případě, že uživatel nechce provádět žádné skenování, nebo se nechce zdržovat, může jednoduše zadat SSID sítě a spustit testování. Nástroj se pokusí ověřit, jestli je daná síť v dosahu. Pokud není, pokusí se alespoň k ní připojit.

5.2 Nastavení programu

Protože nástroj může pracovat s jakýmkoliv bezdrátovým rozhraním, včetně externích sond, je potřeba vybrat rozhraní, se kterým má nástroj pracovat. Obrázek sondy se nachází v příloze C. V nastavení lze tedy vybrat jak rozhraní ze seznamu dostupných, tak zadat název ručně. Pokud se jedná o externí sondu, nastaví se místo názvu IP adresa a port, po kterém se má se sondou komunikovat. V základním nastavení se použije rozhraní, které je první v seznamu dostupných.

5.3 Výpočet vhodného kanálu

Zvláštní částí implementace bylo vymyšlení a realizace algoritmu, který má za úkol kontrolovat kanál. Algoritmus zkontroluje aktuální kanál a popřípadě vybere nejvhodnější, který doporučí uživateli. Základem je obrázek, který ilustruje frekvenční pásmo standardu 802.11 s kanály.



Obrázek 5.1: Grafické znázornění kanálů

Z tohoto poznatku lze odvodit několik základních informací. Frekvenční pásmo je rozděleno do 13 kanálů (pro Evropu). Kanály 1, 6 a 11 jsou nezarušené. Dle grafu je vidět, že mimo tyto kanály se zbytek kanálů zarušuje mezi sebou. Například kanál 8 dosti ruší 7 a 9 kanál, ovšem na 10 kanál již nemá téměř žádný vliv. Tyto poznatky jsem využil při vytváření daného algoritmu.

V první fázi dojde ke kontrole kanálu, na kterém se nachází testovaná síť a porovná se s ostatními naskenovanými sítěmi v dosahu. Pokud se síť nachází na kanálu, kde žádná jiná není a to ani v nejbližším okolí (vyjímkou jsou nezarušené kanály), algoritmus vyhodnotí kanál jako správný. Jestliže některá podmínka nesouhlasí, prohledají se veškeré kanály a zjistí se jestli není volný jiný kanál. Nejvyšší prioritu mají opět nezarušené kanály. Pokud ty nejsou volné, pokračuje se vyhledáním kanálu, který nemá ve svém nejbližším okolí jinou síť. Když taková existuje, zobrazí se jako výsledek. Ale pokud ani zde se žádný takový kanál nenajde, tak se doporučí všechny sítě, které jsou volné. Když ani to není možné, vypíše se varování, které o této skutečnosti informuje uživatele. Mezi doporučeními je buď přejít na 5Ghz pásmo, použít vyšší zisk antény, nebo vybrat kanál, na kterém je síť s nejslabším signálem.

Možností, jak daný problém vyřešit, je samozřejmě více. Záleží ale na administrátorovi, jak problém se zarušením vyřeší. Doporučení se zobrazí jak v informačním okně, tak v okně, které obsahuje souhrnné informace o testech.

5.4 Testy

Hlavní částí implementace bylo vytvoření testů, které mají zjistit úroveň zabezpečení sítí. Před samotnou implementací, bylo potřeba jednotlivé typy útoků důkladně nastudovat. Každý test se musel prověřit, zda je opravdu funkční a poté z těchto podkladů začít implementovat. Samotná implementace tudíž zabrala pouze zlomek z celkového času, věnovaného při tvorbě testů. Průběh testování je zobrazen na grafu 5.2.

Security checklist

Volně přeloženo do češtiny "Seznam hodnotící zranitelnost Wi-Fi sítí"[15]. Jak již z názvu vyplývá, jedná se o seznam úkolů, který v případě splnění sníží zranitelnost bezdrátové sítě. Seznam se rozděluje do základních 6 kategorií, z nichž se větví na další podkategorie.

První kategorie kontroluje zarušení okolo bezdrátové sítě. Kontrolují se kanály, síla signálu a další. V druhé kategorii se kontroluje zarušení jinými prostředky, jako jsou mikrovlnné trouby, bluetooth, či jiná zařízení pracující na frekvencích 2,4GHz a 5GHz. Ve třetí kategorii se testuje vlastní access-point, aktuálnost firmwaru, zabezpečení administrace, zabezpečení sítě, případně další možnosti. Testování vlastní stanice je názvem čtvrté kapitoly. Kontroluje se od typu operačního systému, po zabezpečení při sdílení souborů. Pátá kategorie má za úkol kontrolu WLAN infrastruktury a šestá doporučuje uložit veškerá doporučení, plynoucí z toho seznamu.

Tento checklist je základní kostrou celého testování. Podle daného pořadí dochází k postupnému ověření vlastností dané sítě, a to nejen z bezpečnostního hlediska. Případné nedostatky nástroj vyhodnotí po ukončení testů.

Informační okno

Nástroj je navržen pro testování, které může trvat delší dobu. Od takové aplikace se očekává zobrazení užitečných informací, aby bylo poznat, co se právě odehrává. K tomuto účelu je zde informační okno, ve kterém se průběžně během testování zobrazují důležité informace. Ke každé zprávě se připojí časová značka, aby bylo hned poznat, jak dlouho jaká fáze testu trvala.

Samotné testy

Každý test je implementován samostatně a má pro sebe vyhrazenou metodu. Implementace je tudíž jednoduše modifikovatelná. Většina testů využívá implementované testy, které jsou součástí balíku *Aircrack-ng*.

Pro správné provedení testu je potřeba běžně i 7 terminálů, na kterých na každém běží jiná část operace. Toto vše provádí nástroj sám během testování bez vědomí uživatele. Je tedy naprosto běžné, že ve chvíli kdy probíhá testování je aktivní druhé vlákno, aby nedošlo k zamrznutí GUI. V tomto vlákně může naráz běžet např. 5 synovských procesů, které ve smyčce provádějí potřebné kroky pro správné testování sítě.

Další testy po nalezení hesla

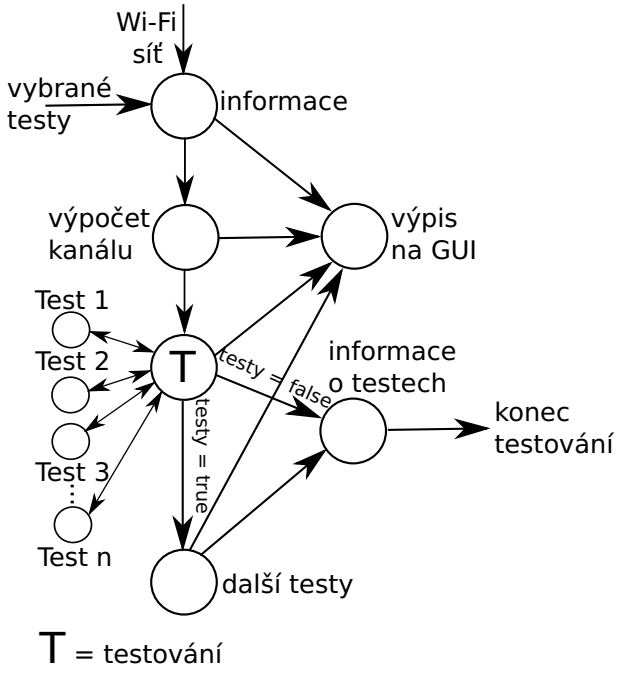
Úspěšné prolomení zabezpečení sítě, neznamená konec testů. Následují další fáze, které prověří bezpečnost uvnitř sítě. Nástroje se pomocí nástroje *wpa_supplicant* připojí do sítě. Zažádá o IP adresu a pokud ji dostane, může pokračovat dále. Pokud není na síti aktivováno

dynamické přidělování IP adres, zobrazí se okno, ve které nástroj zažádá uživatele o zadání IP adresy ručně.

Po úspěšném připojení nástroj prověří bezpečnost i uvnitř sítě. Odhalí se tak další nedostatky, na které spousta administrátorů zapomíná a které by mohl útočník zneužít. Spustí se nástroj *nmap*, který zjistí informace o připojených klientech z celé podsítě, jako je používaný operační systém a otevřené porty. Lze tak nalézt další bezpečnostní díry, například nezabezpečený http port na serveru a další.

Informace o testech

Po úspěšném dokončení testování dochází k další fázi, která má na starosti zobrazení informací o testování. Jedná se o užitečný souhrn informací, který je určen hlavně pro administrátory sítí. Dozví se z nich informace o síti, doporučení vhodného kanálu, průběhy a výsledky testů a následná doporučení pro zvýšení úrovně bezpečnosti. Výpis ulehčuje práci uživateli aplikace, který během testování nemusí sledovat zprávy z informačního okna, ale může si přečíst celý souhrn až po ukončení testování. Informace se vypíšou do nového okna, které se zobrazí nad nástrojem.



Obrázek 5.2: Graf průběhu testování

Vytvoření linuxové distribuce

Finální fází po dokončení implementace a testování, bylo přesunutí nástroje do distribuce BackTrack. Po dalším otestování a doladění posledních detailů došlo k vytvoření Live linuxové distribuce, čímž se splnil jeden z bodů zadání.

Závěr implementace

Po kvalitním návrhu již nebyl takový problém s implentací. Několik problémů se vyskytlo, které jsou popsané výše, ale nic závažného či neobvyklého. Implementace probíhala hladce a vždy se postupovalo po určitých částech. Nejvíce času zabrala samotná studie. Z implementace to bylo testování a interaktivní režim, který byl dost problémový.

Po implementaci se vývoj přesunul do fáze testování, kterou popisuje následující kapitola.

Kapitola 6

Shrnutí a testování

V této kapitole se popisuje fáze testování a celkové shrnutí výsledků. Již od začátku implementace probíhalo částečné testování hotových částí nástroje. Testy měli za úkol odhalit případné nedostatky a chyby. Při implementaci testů bylo samotné testování rozděleno do několika fází.

1. Studium testů - V první fázi bylo potřeba nastudovat potřebné informace a materiály pro pochopení funkcí a používání potřebných nástrojů.
2. Testování funkčnosti - Poté, co byly nashromážděny dostatečné znalosti, se začalo s testováním, aby se nástroje vyzkoušely v praxi ještě před samotnou implementací. Při těchto testech docházelo k zaznamenávání poznatků, které byly velmi cenné při implementaci do nástroje.
3. Implementace testů a finální testování - Poslední fází bylo využití získaných poznatků a implementace. Testování probíhalo vždy po částech a poté jako celek. Dále v této kapitole je ukázka dvou testů.

6.1 Nástroj pro testování

Pro uskutečnění testování bylo nutné si pořídit potřebná zařízení.

Jako testovací stanice, ze které se spouštěl nástroj, posloužil můj notebook s integrovanou bezdrátovou síťovou kartou Intel 4965AGN. Problémem bylo, že v mé linuxové distribuci využívá ovladače *iwlagn*, které nepatří mezi zrovna otevřené pro monitor mód, natož injekci paketů. Tento problém je naštěstí vyřešen přímo v Live distribuci, neboť již obsahuje upravené ovladače, a ty problémy nemají.

Další nezbytností bylo pořízení access-pointu, který podporuje všechny běžné standardy zabezpečení. Byl vybrán levný a hodně oblíbený D-Link umožňující snadnou administraci přes webové rozhraní. Bez této komponenty by celá fáze testování byla mnohem složitější.

Poslední, neméně důležitou částí byl mobilní telefon vybaven technologií Wi-Fi. Ten vykonával simulaci klienta, připojeného do sítě a simulující provoz na síti (například stahováním cd Ubuntu).

6.2 Testování sítě zabezpečené šifrováním WEP

Při návrhu nástroje jsem mimo jiné zjišťoval statistiky Wi-Fi sítí v České republice. Bohužel kvalitní studie jsou velmi těžko zjistitelné. Jako nejlepší výzkum jsem vybral od

firmy Ernst & Young [16]. Z jejich průzkumu vyplývá, že ze všech testovaných Wi-Fi sítí v Praze, bylo celkem 84% sítí zabezpečených. Ovšem z těchto 84% bylo celých 58% zabezpečeno šifrováním WEP. Procento je to opravdu vysoké vzhledem k tomu, že se jedná o velmi zastaralé šifrování, které je jednoduše prolomitelné.

Jako první příklad uvádím testování sítě zabezpečené šifrováním WEP. Snímky testu se nacházejí v příloze A. Za vhodný typ testu si vyberu PTW [17], což je upravený Klein útok pro WEP. Test patří mezi základní na WEP. Pro tento typ útoku je potřeba zachytit provoz na síti cca. 2 - 50 miliónů inicializačních vektorů (IV), v závislosti na délce klíče a typu IV. Tato skutečnost se objeví během testu v informačním okně pro orientaci uživatele. Dále se v informačním okně dynamicky mění množství zachycených inicializačních vektorů. Proto, pokud si zvolí uživatel tento typ testu a za delší časový úsek není schopen nachytat ani zlomek potřebných IV, nemá smysl dále v testu pokračovat. Po nachytání dostatečného množství se automaticky vypíše informace, že test byl úspěšný a povedlo se najít WEP klíč. Důležitou informací je, že klíč se uživatel nedozví. Administrátor sítě heslo zná a cílem tohoto testovacího nástroje není vytvoření nástroje crackovacího.

Délka šifry	**Klíč**	**Počet IV potřebných k nalezení klíče**
64-bit	heslo	1 500 000 IV
128-bit	bezpecna!!sit	6 000 000 IV
128-bit	WST-PIC16F84A	4 800 000 IV
128-bit	WST-PIC16F84A	8 000 000 IV

Tabulka 6.1: Počet IV a síla šifry k prolomení ochrany WPA

Z tabulky 6.1 je vidět potřebný počet IV ke zjištění klíče. Stejně tak je vidět, že i se stejným heslem je k prolomení potřeba jiný počet inicializačních vektorů. Z toho jednoznačně vyplývá, že nezáleží jak je heslo silné, ale jaké konkrétní IV jsou zachyceny. Což neovlivníme. Jediný způsob jak lze ovlivnit potřebné množství IV je délka šifry, což jednoznačně vyplývá z tabulky.

Jiné typy testů na WEP, které jsou implementované v nástroji, provoz nepotřebují a dokonce ani do sítě připojené klienty nepotřebují. Z těchto informací se dá odvodit nevhodnost šifrovacího algorimtu WEP i na domácí bezdrátové sítě.

6.3 Testování sítě zabezpečené šifrováním WPA2 / TKIP

Jako další příklad uvedu testování sítě zabezpečené šifrováním WPA 2. Snímky testu se nacházejí v příloze B. Jde o typickou ukázku využití silného zabezpečení v kombinaci se slabým heslem. Pro tento typ testu jsem vybral WPA / WPA 2 cracking, které se skládá z několika fází. Heslo v administraci access-pointu bylo nastaveno na „konference“.

První krok po spuštění testu je zachycení WPA/WPA2 handshake. Ten se posílá ve chvíli, kdy se připojuje klient do sítě. Bezchybné provedení této fáze je pro test zásadní. V 2 fázi testu dojde k deautentizaci klienta a ve třetí se spustí 4-fázový slovníkový útok.

Slovníkový útok se neprovádí na síti, nýbrž vše probíhá již na stanici, tudíž je tento brute-force útok velmi rychlý. První slovník obsahuje 500 nejhorších hesel uvedených v knize Perfect Password. [18]. V druhé fázi se testuje 3000 nejčastěji používaných hesel v polovině 60-tých let na unixových stanicích. Ve třetí fázi je český slovník složený přibližně z 270

000 slov a v poslední to je anglický slovník o velikosti přibližně 300 000 slov. Každá část se provádí zvlášť a informace, jaká fáze právě probíhá i výsledky, se postupně zobrazují v informačním okně.

Z dodatečných testů vyplývá, že tento test byl úspěšný ve 3 fázi slovníkového útoku. Od spuštění první fáze slovníkového útoku uběhlo 24 vteřin během kterých se první dvě fáze vyhodnotily jako neúspěšné. Výsledkem testování je úspěšně implementovaný slovníkový útok, který během pár minut od zachycení WPA/WPA2 handshake otestoval síť na slabé heslo.

6.4 Souhrn

Důkladným testováním se podařilo odstranit nedostatky při implementaci, které jsou běžnou součástí jakéhokoliv vývoje softwaru. Nástroj je plně přizpůsoben pro použití v běžném provozu. Povedlo se sloučit sedm testů do jediného jednoduchého nástroje, díky kterým zjistí bezpečnostní úroveň dané bezdrátové sítě. Počítá se s možností výskytu dalších nedostatků, jež by následně sloužily jako výchozí body při tvorbě upgradovaných verzí.

Jedná se o největší projekt jakého jsem se zúčastnil a navíc bez týmové spolupráce. Získal jsem velmi cenné zkušenosti při vytváření nástroje, které jistě zužitkuji v praxi. Já sám vidím v tomto nástroji velký potenciál. Pokud bude zájem ze strany uživatelů, rád bych pokračoval v dalším vývoji nástroje. Jako licence byla zvolena verze GPL.

Nástroj jsem již několikrát sám využil pro zjištění úrovně zabezpečení konkrétní bezdrátové sítě. A jelikož analýza bezpečnostní úrovně sítě vyžaduje mnoho času a práce, nástroj WST může admistrátorům sítě tento čas ušetřit.

Kapitola 7

Další možnosti rozšíření

Kapitola pojednává o možných rozšířeních nástroje WST do budoucna. Vylepšení uživatelského rozhraní, upgrade testů, lepší formulování výpisů a podobně.

Uživatelské rozhraní

V uživatelském rozhraní by bylo možné udělat několik úprav.

- Celkové vylepšení grafiky. Více grafických efektů pro přehlednější používání a modernější design.
- Vylepšené zobrazení skenovaných sítí, Více informací o sítích.
- Přehlednější výpisy v informačním okně. Animované ukazatele činnosti testování.

Úprav uživatelského rozhraní lze udělat velké množství. Toto jsou jen ty nejzákladnější, které by nástroj vylepšily z pohledu použitelnosti a přehlednosti.

Nastavení programu

Stávající možnosti nastavení jsou značně omezené. Toto jsou další možná rozšíření pro lepší přizpůsobení nástroje:

- Možnost nastavení časového intervalu pro obnovování informací u interaktivního módu.
- Ukládání výpisu testování do souboru.
- Možnost uložení / nahrání aktuálního nastavení např. na flash disk. Při častějším spouštění pouze nahrát nastavenou konfiguraci.

Testování sítí

Testování sítí může být také vylepšeno o několik možných rozšíření

- Možnost jednoduché editace a úpravy slovníků při slovníkovém útoku.
- Vybrání pouze těch testů, které se hodí na daný typ zabezpečení.
- Odhadnutí IP adresy ze zachytnutých paketů po připojení do sítě a vypnutém DHCP.

Kapitola 8

Závěr

Aplikace, která má za úkol testovat bezpečnost Wi-Fi sítí, má dle mého názoru velký potenciál. Nástroj podobného typu jsem nikde nenašel. Může se hodit běžným uživatelům, kteří nevědí, jak bezpečně nastavit svou domácí síť, ale mohou ji využívat i profesionální administrátoři pro dostatečné zabezpečení podnikových Wi-Fi sítí. Těsně před odevzdáním práce vyšla nová verze BackTracku, nástroj jsem tedy implementoval přímo do ní. Zaručí se tak maximální aktuálnost veškerých nástrojů.

Aplikaci jsem implementoval úspěšně a splnil tak veškeré stanovené požadavky. Snažil jsem se o využití nejnovějších bezpečnostních znalostí v oblasti bezdrátových sítí. Využití této aplikace je velmi široké a doufám, že bude pro uživatele přínosem. Samozřejmě, že pro úspěšné fungování nástroje bude potřeba jeho aktualizace. Proto jsem se snažil vytvořit celý nástroj tak, aby případné modifikace byly co nejjednodušší.

Literatura

[1] WWW stránky. 'wireless fidelity' debunked. http://www.wi-fiplanet.com/columns/article.php/3674591.

[2] MILLER Stewart S. *Wi-Fi Security*. McGraw-Hill Professional; 1 edice, 2003. ISBN 978-0071410731.

[3] WWW stránky. Ieee-sa -ieee get 802 program [online]. http://standards.ieee.org/about/get/802/802.11.html, 2010 [cit. 2011-03-01].

[4] WWW stránky. Aircrack-ng [online]. http://www.aircrack-ng.org/.

[5] WWW stránky. Top 10 vulnerabilities in today's wi-fi networks - computerworld [online]. http://www.computerworld.com/s/article/72624/Top_10_Vulnerabilities_in_Today_s_Wi_Fi_Networks, 2002 [cit. 2011-05-10].

[6] WWW stránky. Wep (wired equivalent privacy). http://www.networkworld.com/details/715.html, 2006 [cit. 2011-05-05].

[7] WWW stránky. Airsnort homepage [online]. http://airsnort.shmoo.com/.

[8] WWW stránky. Šifrování wpa lze prolomit nejen hrubou silou. http://securityworld.cz/aktuality/Sifrovani-WPA-lze-prolomit-nejen-hrubou-silou-1345.

[9] WWW stránky. Specification for the advanced encryption standard (aes). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001 [cit. 2011-05-10].

[10] WWW stránky. Wpa/wpa2 tkip attack. http://www.airtightnetworks.com/home/resources/knowledge-center/wpa-wpa2-tkip-attack.html.

[11] Md Sohail Ahmad. Wpa too! [online]. http://defcon.org/images/defcon-18/dc-18-presentations/Ahmad/DEFCON-18-Ahmad-WPA-Too-WP.pdf, 2011-01-1 [cit. 2011-01-21].

[12] WWW stránky. Backtrack linux - penetration testing distribution. http://www.backtrack-linux.org.

[13] WWW stránky. Qt - a cross-platform application and ui framework. http://qt.nokia.com/products.

[14] WWW stránky. Qt 4.7: Qthread class reference. http://doc.trolltech.com/latest/qthread.html#details.

[15] Phifer LISA. Wi-fi vulnerability assessment checklist [online]. http://searchnetworking.techtarget.com/feature/Wi-Fi-vulnerability-assessment-checklist, 2006 [cit. 2011-03-02].

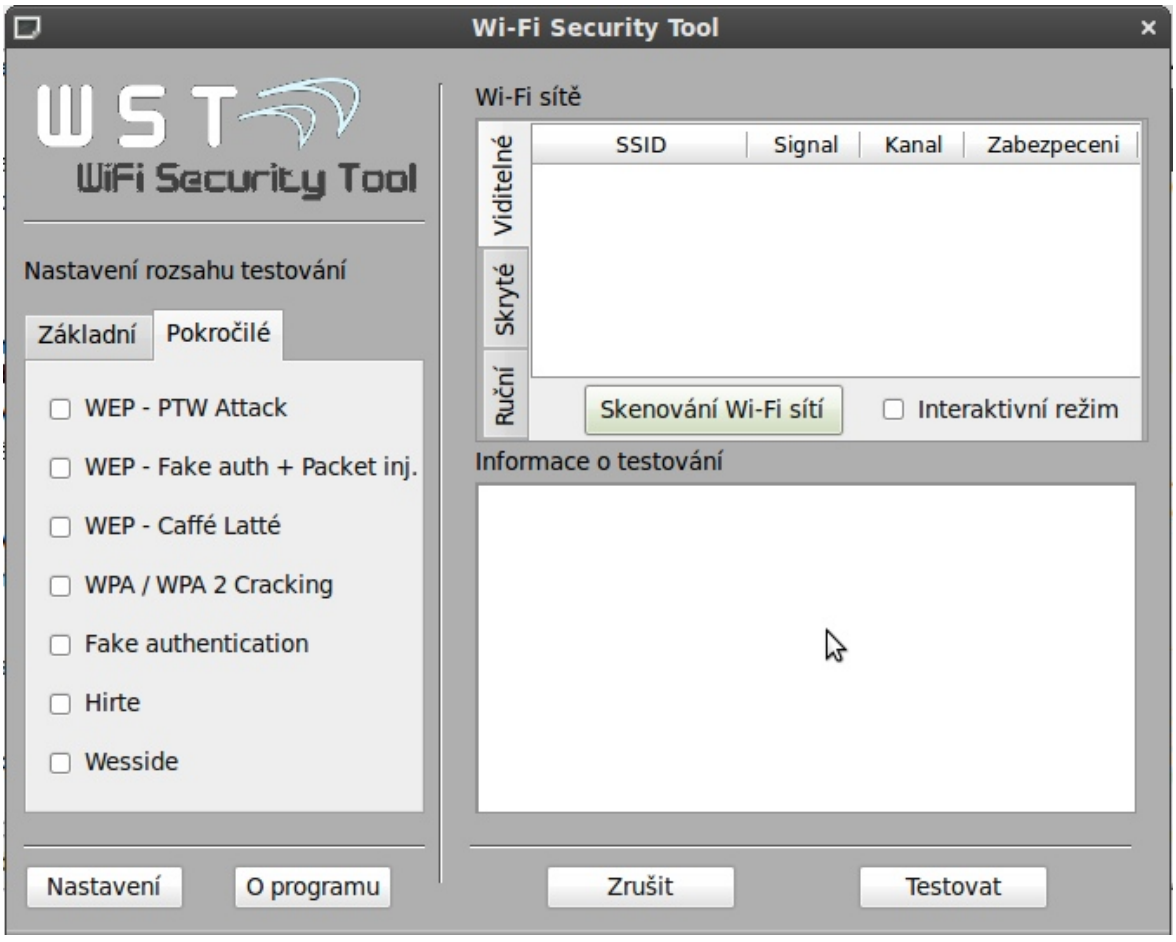
[16] EYGM Limited. Průzkum bezpečnosti bezdrátových sítí v praze a bratislavě [online]. http://www.ey.com/Publication/vwLUAssets/2009_v_bezpecnosti_brozura/$FILE/7544_EYcr_Wifi%20Survey%202009%2004%20new%20lock.pdf, 2009 [cit. 2011-05-05].

[17] WWW stránky. Aircrack-ptw. http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/.

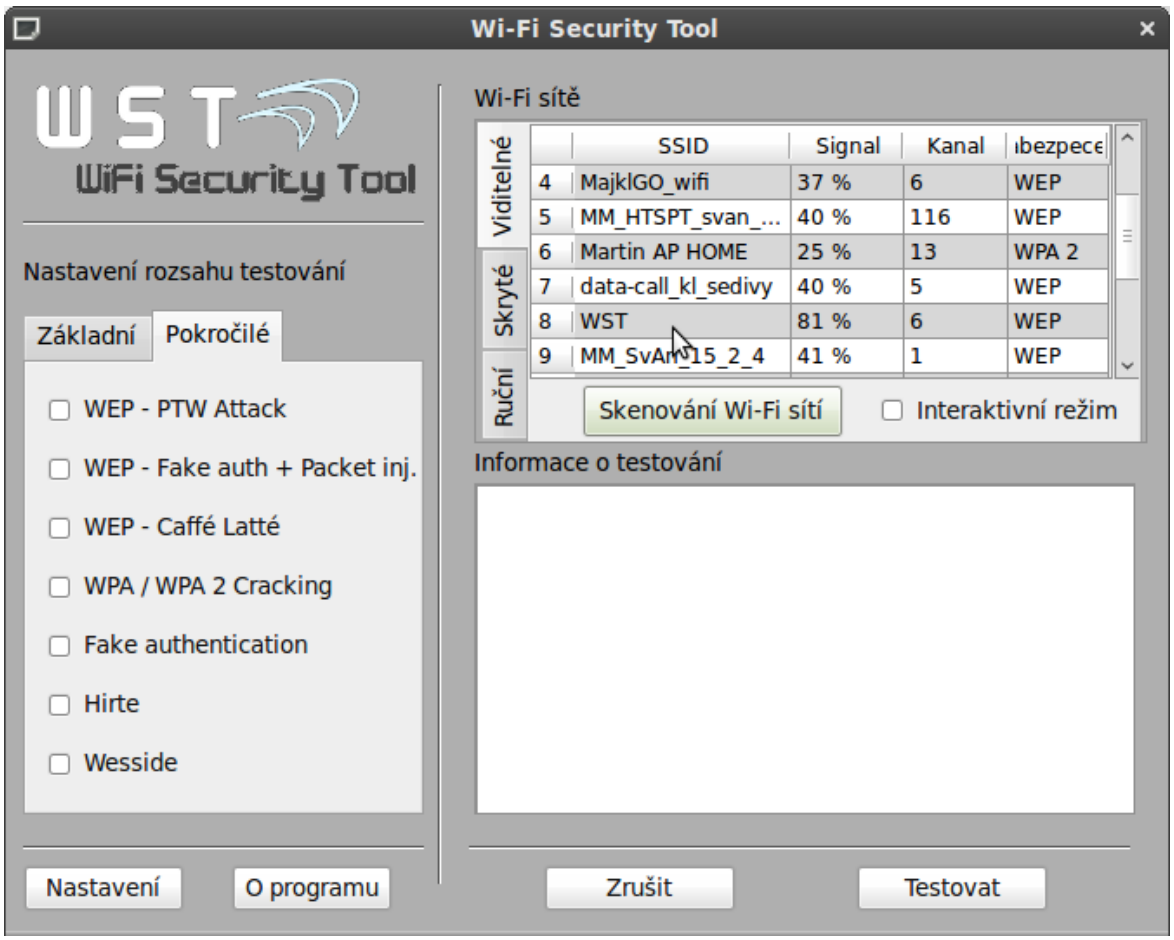
[18] BURNETT Mark. *Perfect Password : Selection, Protection, Authentication.* Kanada : Syngress, 2005. ISBN 978-1597490412.

Příloha A

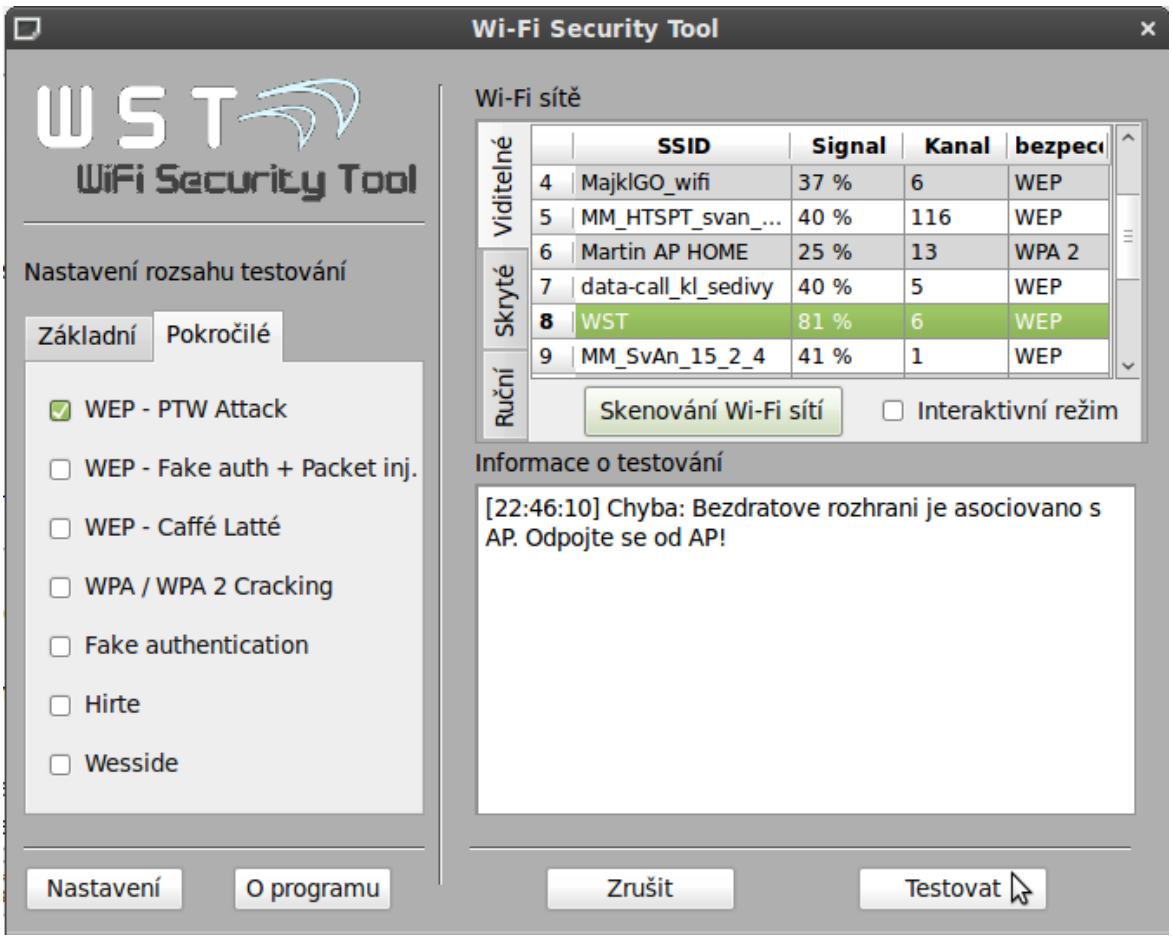
Ukázka testu na síť zabezpečenou šifrováním WEP



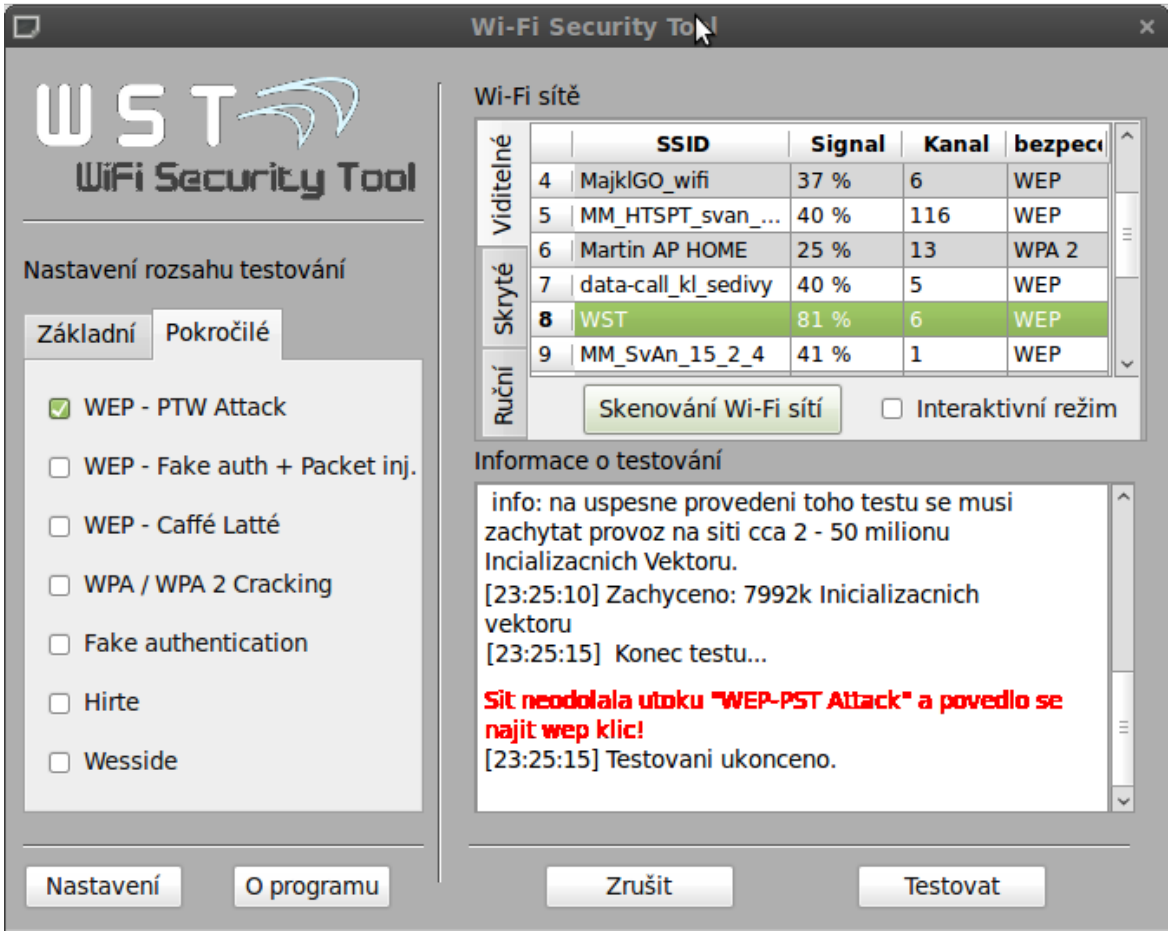
Obrázek A.1: Spuštění nástroje



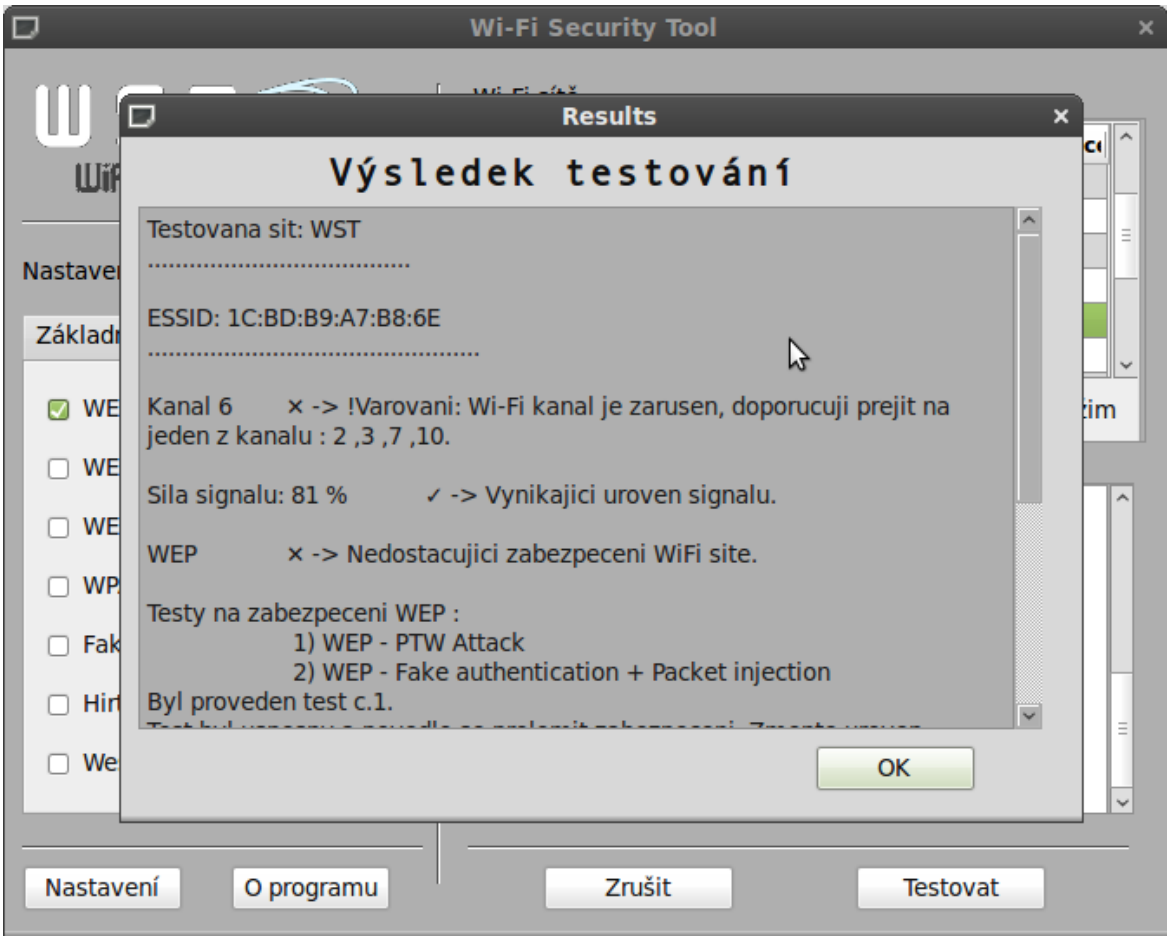
Obrázek A.2: Skenování Wi-Fi sítí



Obrázek A.3: Chyba při spuštění testů



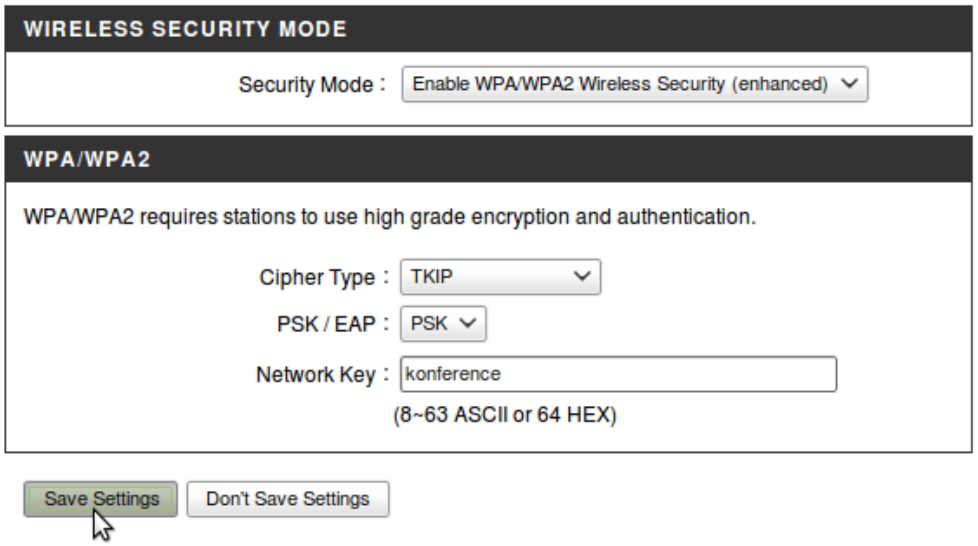
Obrázek A.4: Prolomení ochrany



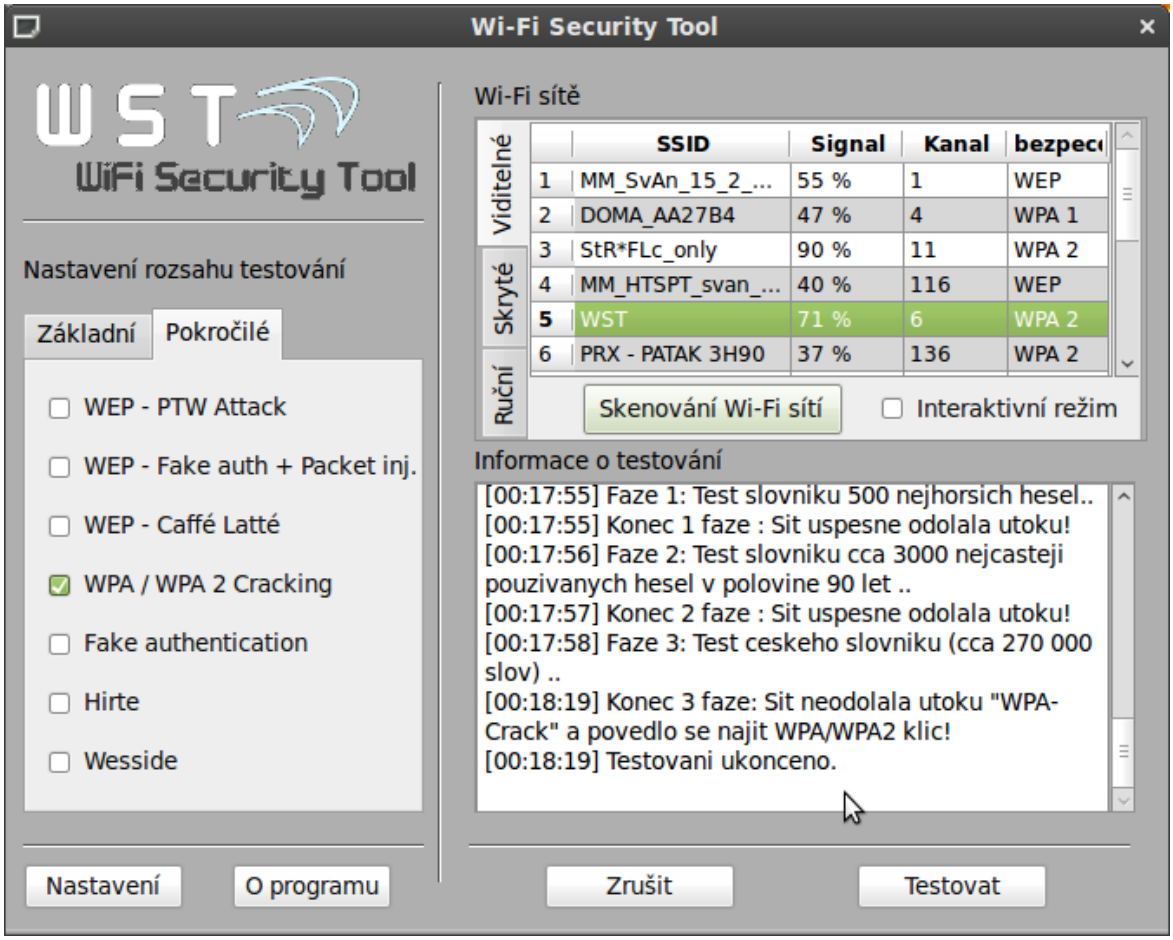
Obrázek A.5: Vyhodnocení testování

Příloha B

Ukázka testu na síť zabezpečenou šifrováním WPA 2



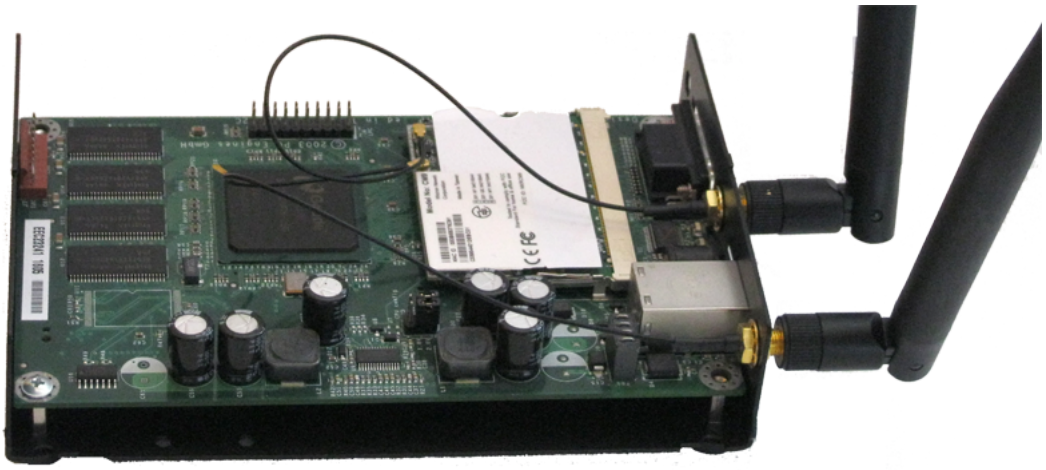
Obrázek B.1: Nastavení slabého heslo na administraci AP



Obrázek B.2: Prolomení slovníkovým útokem

Příloha C

Příklad externí sondy



Obrázek C.1: Externí sonda WRAP